Implementation Guide:

Automating multi account permissions management in AWS using CloudKnox and AWS Control Tower
# Table of Contents

- Foreword ............................................................................................................................................................. 3
- Solution overview and features .......................................................................................................................... 3
- Architecture diagram ........................................................................................................................................... 3
- Deployment and Configuration Steps ................................................................................................................. 4
  - Step 1: CloudKnox - Initial Setup ..................................................................................................................... 4
  - Step 2: AWS Setup - AWS Control Tower management account ................................................................. 6
  - Step 3: Test – Create or Enroll AWS Control Tower managed account .................................................... 6
  - Step 4: View the CloudKnox AWS (Overview) Dashboard ........................................................................ 6
- Solution Estimated Pricing ................................................................................................................................... 7
- FAQs ..................................................................................................................................................................... 7
- Additional resources ............................................................................................................................................ 7
- Partner contact information ................................................................................................................................. 7
Foreword

CloudKnox Security empowers security and cloud infrastructure teams to protect their cloud resources from the misuse or exploitation of identity permissions by delivering a platform that enables the continuous enforcement of least privilege policies across all AWS accounts in the organization.

This Implementation Guide describes how AWS Marketplace customers can activate CloudKnox permission management capabilities automatically when creating new accounts with AWS Control Tower.

Solution overview and features

By bringing together data from every account in your company’s AWS environment CloudKnox provides a continuous and adaptive framework for viewing, detecting, and remediating over-permissioned human and non-human identities. Through a risk-based decision-making approach, security operations, and cloud infrastructure teams can continuously create, monitor, and enforce least privilege policies across all AWS accounts in a single dashboard. This ensures every identity that can access cloud infrastructure, including employees, third party contractors, service accounts, bots, applications, application programming interfaces (APIs), keys and cloud resources such as Amazon Elastic Compute Cloud (EC2) Instances, only have the permissions needed to perform their daily tasks and nothing more.

The solution described in this guide greatly simplifies the process for provisioning CloudKnox in multi-account AWS environments by automatically adding metric and log collection to newly created accounts.

Architecture diagram

The solution is deployed using AWS CloudFormation templates and integrates with AWS Control Tower lifecycle events. When a new account is created, or an existing one is enrolled using the AWS Control Tower Account Factory, the lifecycle event triggers AWS Lambda function. The Lambda function creates a new CloudFormation stack instance in the vended account, creating the required AWS Identity and Access Management (IAM) role in the newly vended account.

The stack instance also configures CloudKnox to use the IAM role to collect account data from IAM, resource id/tags, and AWS CloudTrail logs from the new account. See the documentation here for more details.
Pre-requisites

To leverage the solution, you will have to:

- Have an AWS Account with AWS Control Tower set up in it, for more information check out the Getting Started with AWS Control Tower section in the AWS Control Tower User Guide

Deployment and Configuration Steps

The solution can be found in the CloudKnox Control Tower GitHub repository. It uses two AWS CloudFormation templates that you will deploy in your AWS Control Tower management account. These templates include all the components required to integrate CloudKnox with new AWS accounts that you create using the AWS Control Tower Account Factory.

Step 1: CloudKnox - Initial Setup

1. Have an existing CloudKnox account or purchase a subscription via the AWS Marketplace from Audit account in your AWS Control Tower environment. Alternatively, you could also subscribe in a Security account if you have a separate account created for security related tasks.
   a. For new users, sign up for an account at https://app.cloudknox.io
c. Choose **Continue to Subscribe**

![CloudKnox Cloud Security Platform](image)

**Overview**

- Pricing
- Usage
- Support
- Reviews

![Configure your Software Contract](image)

**Configure your Software Contract**

Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.

**How long do you want your contract to run?**

- 12 months
- 36 months

**Renewal Settings**

- [Create contract](image)

By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. Your use of AWS services is subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

![CloudKnox Cloud Security Platform](image)

You're purchasing the following contract. When you choose Pay now, your AWS account ID is invoiced. Payment is due when your AWS bill is due. If your usage exceeds your contract, additional usage costs apply.

- **Cloudknox Cloud Security Platform - 12MONTHS Contract**
  - **Auto Renew - No**
  - **$8495.00 - Due Today**

![Pay now](image)

Cancel Pay now

You will be redirected to [https://app.cloudknox.io](https://app.cloudknox.io). Login using account you registered in step 1.a.

Click Deploy on main page and follow instructions to download CloudFormation Template and create an EC2 instance sentry on Audit or Security account in your AWS Control Tower environment. It is not recommended to launch EC2 instance on Management account.

h. Complete instructions to enter PIN and register the newly created agent.
2. Log in to the CloudKnox API Integrations console and click on Generate New Key. Make a note of the generated Access Key, Secret Key and Service Account ID for use in Step 2 below.

Step 2: AWS Setup - AWS Control Tower management account

1. Set up the AWS Control Tower Account Provisioning Automation for CloudKnox.
   a. Launch the `aws-cloudknox-controltower.yml` template.
      i. Enter the AWS Account ID of the Audit account where sentry is installed in Step 1.1. Change the role name if it is different from default role name
      ii. Enter the Access Key, Secret Key and Service Account ID generated in Step 1.2.
      iii. Accept the default values for remaining parameters:
         1. URL is to be changed only if CloudKnox login is not app.cloudknox.io
         2. API id is unique value not changed unless notified by CloudKnox
         3. CloudKnox template URL is default unless customization was done in local environment

Step 3: Test – Create or Enroll AWS Control Tower managed account

- From the AWS Control Tower Management Account:
  - Use Account Factory to create a new account or enroll an existing one
  - This can take up to 30 mins for the account to be successfully created and the AWS Control Tower Lifecycle Event to trigger
- Log into the AWS Control Tower managed account:
  - Validate that a CloudKnox Integration Role (`IAM_R_KNOX_SECURITY_XA` IAM role) has been created in the managed account. This is a cross-account Role where the trusted account ID – sentry account ID

Step 4: View the CloudKnox AWS (Overview) Dashboard

- Log into your CloudKnox account.
- Click on data sources page to see data collector is in Collecting state for an additional account
- View CloudKnox console to view analytics of newly created account. It could take couple of hours for data polling of a new AWS account.
Solution Estimated Pricing

Contact CloudKnox team to learn more.

FAQs

You can find a list of FAQs for the CloudKnox AWS Integration in our documentation here.

Additional resources

- CloudKnox AWS Solutions page
- CloudKnox AWS Integration documentation

Partner contact information

For general inquiries, contact info@cloudknox.io.